10/542500

HOEFER & PARTNER

Sony DADC Austria AG

JC20 Rec'd PCT/PTO 1 5 JUL 2005

SON040101PCT

16.01.2004

Secure WEB Access via an Original CD

Description

The present invention relates to a method for securing an access to a predetermined area of a target server, a method for starting a secure access to a
5   predetermined area of a target server, and a record carrier.

To achieve a better position in the market and to better satisfy customers, today's CD and/or DVD labels, i.e. producers, want to offer added value and bonus material (in the following only referred to as bonus material) to a CD
10 content and/or DVD content to the customers. A convenient way is to offer such services via the internet. However, such a system to offer bonus material must be secured to legitimate buyers of a respective record carrier, which might also include CD-ROMs or other current or future record carriers.

15 Therefore, currently secure internet connections that can be accessed with key-codes are offered to customers to access such bonus material. The key-codes are generally serialized e.g. on the data set and have to be entered during a login procedure on a login page to enter predetermined protected areas. The applicant's European patent application 02 003 465.8 "Method and Device for
20 supplying of a Data Set stored in a Database", filed on February 14, 2002, which content is herewith included into this application, describes such a system. The disadvantage of such a method is that the key-codes can be shared and the user experience/convenience suffers.

25 Therefore, it is the object underlying the present invention to provide an improved system to offer bonus material to a legitimate customer of a record carrier.

According to the present invention, this object is solved by a method for
30 securing an access to a predetermined area of a target server as defined in independent claim 1, a method for starting a secure access to a predetermined area of a target server as defined in independent claim 5, and a record carrier as defined in independent claim 20. Preferred embodiments of the methods and record carrier according to the present invention are defined in the respective
35 dependent claims. A computer program product according to the present

invention is defined in claim 18 and a computer readable storage means is defined in claim 19.

The method for securing an access to a predetermined area of a target server
5   according to the present invention comprises the step of providing an information file on a copy protected record carrier, which information file comprises a project identifier and/or an address of an authentification server with which an application using said information file can communicate so that the authentification server can initiate and confirm a connection between a
10   computer on which said application is started and said predetermined area of said target server that is identified by the authentification server and/or the project identifier.

Further, the method for starting a secure access to a predetermined area of a
15   target server according to the present invention comprises the step of accessing of an information file on a copy protected record carrier, which information file comprises a project identifier and/or an address of an authentification server with which an application using said information file can communicate so that the authentification server can initiate and confirm a connection between a
20   computer on which said application is started and said predetermined area of said target server that is identified by the authentification server and/or the project identifier.

Finally, the record carrier according to the present invention is copy protected
25   and comprises an information file, which comprises a project identifier and/or an address of an authentification server with which an application using said information file can communicate so that the authentification server can initiate and confirm a connection between a computer on which said application file is started and a predetermined area of a target server that is identified by the
30   authentification server and/or the project identifier.

Therefore, according to the present invention the record carrier, e.g. a compact or digital versatile disc with audio and/or video information, comprises an information file, e.g. in a second session, and is copy protected by a generally
35   known or future copy protection, e.g. the today used SecuROM copy protection, as described in the applicants European Patent EP 0 899 733 B1, which content is herewith included by reference. This guarantees that an application that accesses this file, or the information file as said application, can distinguish an

original record carrier from a copy. With the data comprised in the information file the user can securely access the predetermined area on the target server that is preferably an internet server, e.g. the bonus material on a content server of the disc label. Since the data is provided in an executable file or accessible to an

5 executable file, i.e. as an or within an application, that can access an automatic client/server authentification system preferably in a secure manner to grant access to certain target servers, e.g. websites, or areas, it can be secured that no key-codes, URLs etc. can be shared with others, since an access is only possible with the original record carrier in the disc drive. Further, the user

10 experience/convenience is very good, since no complicated interaction, such as the typing of long serial codes, is necessary, but the access can be easily initiated, e.g. by a mouse-click. Preferably, the application opens the standard Web browser of the user/computer with the address of the authentification server and transmits at least the project identifier. The security level is quite

15 high, i.e. as high as the security level of the copy protection.

The application might be provided on the record carrier, and/or on a server, preferably downloadable, and/or on an access-software record carrier, i.e. so that a user can start the execution of the application on the computer. In case

20 the application is provided on the record carrier itself, the information file might be a part of the application and/or the application consist of only the information file that is in this case executable.

The information file comprises the project identifier and/or the address of the

25 authentification server. This information is included according to the used authentification system. E.g. in case only one authentification server exists, the address of the authentification server needs not to be included in the information file on the record carrier, since it can be hard coded in the application that e.g. can be downloaded from a server of the disc label. On the other hand, in case

30 one authentification server exists for every different project, e.g. different CD content, no project identifier needs to be included in the information file, since the address of the respective authentification server alone indicates the predetermined area on the target server. In this case the target server, i.e. content server, and the authentification server might be one physical device that

35 might include further target and/or authentification servers. Of course, in case different authentification servers exist that are designed for authentification of different projects, e.g. one for each disc label that handles all different discs of

that label, the respective address of the authentification server and the project identifier have to be included in the information file.

5   According to the present invention preferably an autorun-information file is provided on said record carrier, which autorun-information file provides an automatic execution of a predetermined executable file after the record carrier is loaded in a reading device.

10   According to the present invention preferably an autostart file is provided on said record carrier, which autostart file gets automatically executed after the record carrier is placed and loaded in a reading device and which autostart file provides a link to start said application, or which autostart file is part of said application, or which autostart file is said information file.

15

According to the present invention preferably the application gets started from said record carrier, or from a server, preferably as a download, or via an access-software record carrier, preferably after an installation of the application on a hard disc of the computer.

20

According to the present invention, preferably said application verifies whether or not the record carrier is an original and performs said communication with said authentification server in case of a positive verification.

25   According to the present invention preferably said executable file transmits a changing parameter of the computer, in particular a randomly generated number and/or a computer system time to said authentification server.

According to the present invention, additionally or alternatively preferably said
30   authentification server verifies whether or not the communication with said application and/or a transmission of said project identifier as a request for a connection between said computer and said predetermined area of said target server is posted from said application and initiates a connection of said computer with said predetermined area of said target server in case of a positive
35   verification. This verification might be performed on basis of an encryption/decryption scheme used to secure the information that is communicated between the application and the authentification server or parts thereof.

According to the present invention, said authentification server further additionally or alternatively preferably verifies whether or not a changing parameter of the computer, in particular a randomly generated number and/or a
5   computer system time transmitted from said computer, was not already previously used and initiates a connection of said computer with said predetermined area of said target server in case of a positive verification.

According to the present invention, preferably after a positive verification a
10   connection between said authentification server and said target server is set-up by said authentification server that connects to said target server to secure that the computer is connected to said predetermined area of said target server via said authentification server.

15   According to the present invention, in this case, preferably
         - the authentification server generates a session identifier based on the positive verified values and transmits said session identifier to said target server via said connection between said authentification server and said target server,
         - said connection between said computer on which said application is
20   started and said predetermined area of said target server is set up by redirecting the connection between the computer and the authentification server to the target server or by forwarding data of the protected area to the computer, and
         - said connection between said computer on which said application is started and said predetermined area of said target server is executed after the
25   target server received a confirmation of a validity of the session identifier from the authentification server. The forwarding of data of the protected area to the computer might include that data needed to establish a connection between the computer and the target server is forwarded so that such a connection might be set-up from the computer side or that data that the computer user requests, e.g.
30   contents of the target server, are forwarded, i.e. the computer only communicates with the authentification server that communicates with the target server.

According to the present invention the validity of the session identifier is preferably confirmed by the authentification server by positively determining
35   whether or not the session identifier exists and/or whether or not the session identifier was already requested to be valid.

According to the present invention the target server preferably assigns a temporary session cookie to the computer so that the whole predetermined area of the target server can be accessed via said connection between said computer on which said application is started and said target server

5

According to the present invention preferably said record carrier is copy protected by copy protecting the information file.

10   According to the present invention preferably said predetermined area on said target server comprises bonus material of the content that is included on the record carrier besides said executable file, e.g. a video to a song included on the record carrier.

15   According to the present invention preferably said information file is a part of said application or is an executable file of said application.

The computer program product according to the present invention comprises computer program means adapted to perform the method steps as set-out above 20   or parts thereof when being executed on a computer, digital signal processor, or the like.

The computer readable storage means according to the present invention comprises a computer program product according to the present invention.

25

All different aspects of the present invention as set-out above and further elucidated below might be combined in any way. The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an embodiment of the invention and, together with a general description of the 30   invention given above, and the detailed description of the embodiment given below, serve to explain the principles of the invention, wherein:

Fig. 1   shows an embodiment of an environment to offer bonus material and added value according to the present invention,

35   Fig. 2   shows a functionality description of the embodiment shown in Fig. 1, and

Fig 3   shows a flow chart of the authentification server and the target server according to an embodiment of the present invention.

The environment to offer bonus material and added value as shown in Fig. 1 allows to restrict the access to predetermined areas and services offered on a website to only owners of a particular, copy protected record carrier, e.g. CD 1.

5   Copy CDs 7 of the original CD1 will not provide the access, since the copy might not be accessible e.g. in case of a copy protection of the whole CD, or the executable file that provides the access according to the present invention which is provided on the original CD 1 is not copied due to a copy protection of this file, or original and duplicate are distinguishable due to their behaviour and the

10   environment offers the bonus material only to originals, i.e. generally since the executable file or the whole CD 1 is copy protected. Therefore, only a buyer of the original CD 1 has access to bonus material, such as video streams, music downloads, games, price reductions in online shops, and so on.

15   Once the user has inserted the original CD 1 into a computer 2, an access of a portal 3 that offers the bonus material and/or the additional services is possible e.g. via the internet 4. The shown portal 3 offers an authentification 3a after which bonus material 3b, push services 3c, and mobile services 3d are available. Further, community services 3e, customer relationship 3f, and games/chat 3h

20   are offered as well as an information window 3g. Via the portal 3 the verified user can access media rich content from an online digital production library 5 and can communicate via a MM-Message Service Centre 6 with a wireless network. The bonus material 3b, community services 3e, customer relationship 3f, and games/chat 3h might be internet services, the push services 3c might be

25   directed to the internet, e.g. e-mail, or to mobile phones or smartphones, e.g. short message service. The mobile services 3d might be directed to mobile phones or smartphones.

The added value offered to the customer, i.e. the owner of the copy protected CD

30   1 according to the present invention, is protected intellectual property of the artists and publishers, e.g. music or video publishers, since tethered services are only available through the original record carrier. Further, the convenience and quality expected is provided which is a prerequisite to keep consumers away from p2p networks. Also, the tracking of user behaviour is possible so that

35   one2one relationships, i.e. profiles, might be build up. The portal 3 might also serve as an extended platform for marketing activities and it bridges the gap between physical/electronic and mobile content delivery. The portal 3 might further show a build in DRM functionality for the major software players, such

as the Real & Windows Media Player, which offers a convergence of media, e.g. CD/internet/mobile devices. An individual feedback according to a listing of preferences is possible and the community aspect might be satisfied by offering chats, games and downloads.

5

Fig. 2 shows an overview of the functionality of the environment shown in Fig. 1. The CD 1 comprises a SecuROM copy protected executable file, which secures that a user that executes the file is the legitimate owner of the CD 1. The executable file is the executable information file as set-out above, i.e. combines

10 the executable file of the application and the information file. The executable file opens the standard browser 8 of the user with the address of the authentification server 9. At least a project identifier that corresponds to the predetermined area that comprises the bonus material etc. is also communicated to the authentification server 9, since in this case one authentification server

15 handles several projects. Preferably, also a computer identifier is transmitted to the authentification server 9 to automatically identify a user.

The authentification server 9 verifies whether the request that is posted by addressing the authentification server 9 and communicating the project

20 identifier is posted by the executable file and in case of a positive verification redirects the browser to the target address that corresponds to the target area so that the portal 3 of the target server or predetermined area of the target server is displayed. The authentification server 9 determines the target address from the project identifier. While redirecting the browser, the authentification server 9

25 communicates with the target server or predetermined area of the target server to secure that the user accesses the services via the authentification server 9.

The original record carrier, here the CD 1, might not only comprise the normal content, e.g. audio and/or video, and the executable file that provides the

30 address of the authentification server and the project identifier, but also a file "autorun.inf" and a file "start.exe". The file autorun.inf secures an automatic loading of the file start.exe after the record carrier is placed and loaded in the drive and the file start.exe is an application that generates a preferably graphical user interface, which offers different possibilities of services related to

35 the record carrier such as bibliography, games, etc. and a link to the executable file according to the present invention that provides the address of the authentification server and the project identifier, i.e. that initiates and executes the connection to the secured content.

In a preferred embodiment of the present invention said executable file generates a unique 8 byte computer identifier from the serial number and volume name of the hard disc "C", the checksum of the computer name, and the version of the
5   operating system.

The executable file then opens the standard browser of the user and transmits e.g. the computer identifier, the project identifier and the system time to the authentification server 9 via the query string of the URL of the authentification
10   server 9. This data is preferably key-coded. An example would be:

http://auth.sonydadc.com/auth.go?id=0B2C67B84A8B2C67B84A013FE2013FE 2D676E6...

15   The project identifier is hard coded in the executable file, which means that a new executable file must be generated for every project, e.g. different CD. The authentification server 9 verifies and stores the data as follows:

- decoding of the data string,
20   - verification whether the string was used already, if this is the case then denying the access,
- comparing the system time from the data string with the system times already previously obtained from the user (on basis of the computer identifier), if the new system time is bigger then granting
25   the access, otherwise denying the access,
- generating of a 16 bit session identifier for this access, and
- redirecting the user to the target page, i.e. target area, of the target server, wherein the session identifier is communicated as query string.

30

The right hand side of Fig. 3 shows the communication between the authentification server 9 and the target server to access a secured web page as entry point of said predetermined area of the target server. As described above, in a first step S1 the user gets redirected after the positive authentification to
35   the target server, e.g. a content server of the disc label, to the layout start of the protected page. With the redirecting also the session identifier generated by the authentification server 9 gets communicated to the target server via the query string. Therefore, such a redirecting could be:

http://www.shakira.com/bonus.php?id=KS1757SKD6K9JGAWE...

After it is determined in a following second step S2 that no user session is active, the target server waits for a call from the authentification server 9 in a third step S3 and after the call the protected page directs a request to the authentification server 9 whether or not the session identifier is valid in a fourth step S4 in which the authentification server 9 also communicates a handshake protocol to the target server. The authentification server 9 determines for this verification whether or not the validity of the session identifier was requested earlier, i.e. whether or not the session identifier is still usable, and whether or not the session identifier exists at all. In case no call from the authentification server comes in the third step S3, the target server stops the access. The target server determines in a following fifth step S5 whether or not a communication with the authentification server is executed and in case of a valid authentification server 9 verifies whether or not the user might have access to the protected page in a sixth step S6. In case no valid authentification server communicates with the target server in the fifth step S5, the target server stops the access. In case it is determined in the sixth step S6 that the user might have access, the user session is started in an eighth step S8, otherwise a communication between target server and authentification server 9 is performed in a seventh step S7 to newly log-in the user.

After the user session is started in the eighth step S8 or it is determined in the second step S2 that a user session is already active, the access to the content is given in a following ninth step S9, so that the user might access the whole predetermined area without new authentification. Thereafter the layout of the protected page ends in a tenth step S10.

For comparison, the left hand side of Fig. 3 shows a normal page that has its content directly between the layout start and the layout end.

The executable file according to the present invention that provides the preferably automated access to the authentification server with at least the project identifier allows to easily modify the contents of a web server so that they are only accessible via the execution of the executable file.

To properly perform its functionality, the authentification server might comprise several tables in a database model. One table might store the core data of each project. Among other things, there are stored a project identifier, the hash of this project identifier and the URL where the browser should be linked or redirected to. A further table might store each request from the executable file according to the present invention so that a request can be verified, since no duplicates are allowed, and also for billing purposes. Among other things there are stored the project identifier, the computer identifier, an automatically created numeric counterpart of the computer identifier and an automatically created random session identifier string. Another table might be written from the target server side via an interface. This table protocols the accesses to the protected content, also within a session. The usage of this table is optional. It is necessary in case the number of accesses of one user/computer should be limited to a predetermined amount and no database should be provided on the target server side.